ÇEKİNO BİLGİ TEKNOLOJİLERİ İÇSEL BİLGİLERİN GİZLİLİĞİNİN KORUNMASI VE BİLGİ SUİSTİMALİNİ ÖNLEME POLİTİKASI

Amaç

Bu politika, şirket içinde üretilen, işlenen veya saklanan tüm bilgilerin gizliliğini ve güvenliğini sağlamak, yetkisiz erişim ve bilgi suistimali risklerini en aza indirmek amacıyla oluşturulmuştur. Aynı zamanda, ulusal ve uluslararası yasal düzenlemelere uyumu ve şirketin itibarını korumayı hedefler.

Kapsam

Bu politika; şirketin tüm çalışanları, yöneticileri, danışmanları, iş ortakları, müşterileri ve tedarikçileri gibi tüm paydaşlarını kapsar ve şirket içi ve dışı tüm bilgi varlıklarını, veri tabanlarını, yazılımları ve bilgi sistemlerini içerir.

Genel Önlemler

1. Bilgi Sınıflandırma ve Erişim Kontrolü

- İçsel bilgiler, sınıflandırma sistemine göre belirlenmeli ve yalnızca ihtiyaç duyan yetkili personel tarafından erişilebilir olmalıdır. Bu kapsamda fiziksel ve mantıksal segmentasyon işlemleri yapılmalıdır.
- Bilginin sadece işi gereği bilmesi gerekenlerle paylaşılması esastır ve bu bilgiye erişim, iş gereklilikleri doğrultusunda yetkilendirme süreçleri ile yönetilmelidir. İş süreçlerinin takip edildiği uygulamalar, proje yönetim uygulamaları, İnsan Kaynakları ve Muhasebe uygulamaları gibi şirket içerisindeki bilgi, belge ve veri paylaşılan tüm uygulamalarda bu konuya dikkat edilmelidir.

2. Gizlilik Sözleşmeleri

- İçsel bilgilerin paylaşımı gerektiğinde, ilgili taraflarla gizlilik sözleşmesi (NDA vb.) imzalanmalıdır. Sözleşmeler, bilginin doğası ve ilgili düzenlemelerdeki hususları içermelidir.

3. E-posta Güvenliği ve Uyarılar

- İçsel bilgilerin e-posta yoluyla paylaşılması durumunda, mesajlara gerekli uyarılar eklenmeli ve bu mesajlar özellikle üçüncü taraflara "gizli" etiketiyle gönderilmelidir. İçsel bilgilerin tamamının e-posta ve kurumsal uygulamalarla paylaşılamayacağı konusunda bilgilendirmeler yapılmalıdır.

4. Fiziksel Güvenlik ve Temiz Masa İlkesi

- Ortak yaşam ve ofis alanlarında, özellikle hassas bilgilerin konuşulmaması, notlar şeklinde paylaşılmaması ve fiziksel ortamlarda bilgi güvenliği için gereken önlemlerin alınması sağlanmalıdır. Basılı materyallerin imhası da güvenli yöntemlerle gerçekleştirilmelidir.

5. Proje Çalışmalarında Alınması Gereken İlave Tedbirler

- Proje ile ilgili iletişimlerde, projeye özgü olan ve üçüncü tarafların çıkarım yapamayacağı bir proje kodu kullanımı sağlanması, gizliliğin sağlanması açısından önemlidir.
- Proje grup adresleri oluşturulmalı ve yazışmalar bu adresler üzerinden yapılmalıdır.
- Stratejik projelerde işlem yasağı ve gizlilik yükümlülükleri projeye başlangıç toplantısında ve e-posta ile hatırlatılmalıdır.
- AR-GE süreçlerini ilgilendiren çalışmalarda sadece şirket içerisinden erişilebilir olunması ilkesi benimsenmelidir.

Bilgi Teknolojileri Temelli Önlemler

1. Şifreleme ve Ağ Güvenliği

- Bilgi aktarımı ve saklanmasında güçlü şifreleme yöntemleri kullanılmalı, ağ güvenliği ise güvenlik duvarları ve diğer teknolojilerle korunmalıdır.
- Bilgisayar ve sunucularda verilerin belirli periyotlarla yedeklenmesi ve şifrelenmesi sağlanmalıdır.

- Ağ üzerinde çalışan tüm uygulamaların çeşitli şifreleme yöntemleri ile haberleşmesi sağlanmalıdır.
- Yazılım güncellemeleri ve güvenlik yamaları düzenli olarak uygulanmalı, anti-virüs ve anti-malware yazılımları etkin bir şekilde kullanılmalıdır.
- AR-GE, yazılım ve güvenlik alanlarında çalışan personelin disk şifrelemesi ve/veya benzer uygulamalarla önlem alması gerekmektedir.

2. Mobil Cihaz ve Uzaktan Erişim Güvenliği

- Mobil cihazlar ve uzaktan erişim için güvenlik politikaları belirlenmeli ve bu politikaların uygulanması sağlanmalıdır.
- Yönetimin kritik olarak değerlendirdiği mobil cihazlar için MDM gibi uygulamalar kullanması sağlanmalıdır.

3. Veri Erişimi/Sınıflandırma ve İmha Politikaları

- Tüm bilgi varlıkları, saklama koşullarına göre sınıflandırılmalı ve gerektiğinde güvenli bir şekilde imha edilmelidir. Bu süreçler düzenli olarak gözden geçirilmeli ve güncellenmelidir.
- Kritik veriye erişim için matris oluşturulmalıdır.
- Erişim yönetimini sağlayan ve/veya denetleyen yazılımlar kullanılmalıdır.
- Rol tabanlı erişim ve görevlerin ayrılığı ilkesine uygun kimlik denetimine uygun veri erişimi sağlanmalıdır.

4. Eğitim ve Farkındalık Programları

- Tüm çalışanlar, düzenli olarak bilgi güvenliği eğitimlerinden geçirilmeli ve bilinçlendirilmelidir. Bu programlar, yeni tehditler ve güvenlik önlemleri konusunda sürekli güncellenmelidir.
- Tüm çalışanların belirli periyotlarla siber güvenlik farkındalık eğitimlerinden geçmesi sağlanmalıdır.

- Siber güvenlik eğitim ve farkındalık uygulamaları/programları uygulanmalıdır.
- Yılda en az bir defa siber tatbikat düzenlenmelidir.

5. Olay Yönetimi ve İhlal Bildirimi

- Şüpheli aktiviteler ve güvenlik ihlalleri hızla tespit edilmeli, kaydedilmeli ve ilgili prosedürlere göre bildirilmelidir. İhlal durumlarında etkin bir olay müdahale planı devreye alınmalı ve soruşturma yapılmalıdır.
- Şüpheli aktivite ve bilgilendirmeler için bir SOME (Siber Olaylara Müdahale Ekibi) bulundurulmalıdır.
- SOME Ekibi belirli periyotlarla görev tanımları kapsamında bilgilendirmeler yapmalıdır.
- İhlal neticeleri değerlendirmeli ve ilgili makamlara bildirilmesi gerekiyorsa bu bilgilendirmelerin yapılması sağlanmalıdır.

6. Denetim ve İzleme

- Bilgilerin gizliliği politikalarının ve uygulamalarının düzenli iç ve dış denetimlerle değerlendirilmesi ve güncellenmesi sağlanmalıdır. Denetim sonuçlarına göre politikalar iyileştirilmelidir.
- Denetim bağımsız ve tarafsız denetim kuruluşları tarafından yapılmalı ve sonuçlar gizli şekilde raporlanmalıdır.
- Zafiyet testi ve doğrulama testi gibi testler yapılmalı ve gerekli güvenlik önlemleri alınmalıdır.

Bu politika, Çekino Bilgi Teknolojileri ve güvenli yazılım geliştirme ortamı vizyonuna uygun olarak hazırlanmış olup, içsel bilgilerin korunması ve bilgi suistimalinin önlenmesi için kapsamlı bir çerçeve sunmaktadır. Politikanın etkin bir şekilde uygulanması, Çekino Bilgi Teknolojileri'nin siber güvenlik risklerini azaltacak ve bilgi varlıklarımızın güvenliğini sağlayacaktır.